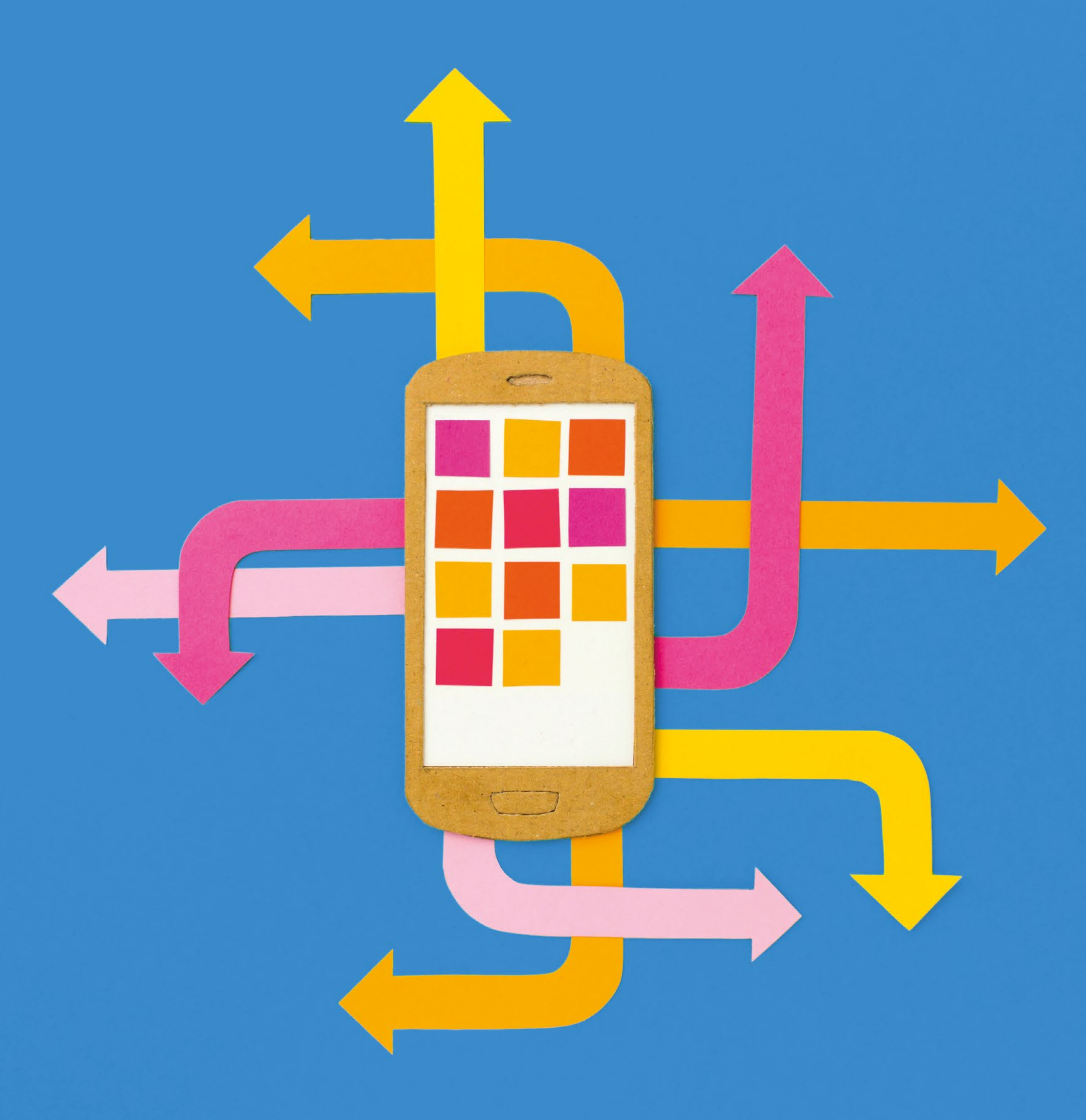
ANDROID SMARTPHONE GOOGLE-FREI EINRICHTEN



SYSTEMLI.ORG

ANDROID SMARTPHONE GOOGLE-FREI EINRICHTEN

!

Einiges in dem Text wird schnell veraltet sein. Wir werden versuchen, die Online-Version aktuell zu halten. Diese findet ihr unter https://wiki.systemli.org/howto/android/setup

Nach dem Entfernen der Google Services wird die eine oder andere Funktion anders oder gar nicht mehr funktionieren. Ohne Google Services wird man weder die Echtzeit-Stauanzeige von *Google Maps*, noch personalisierte Suchergebnisse bekommen. Aber für die meisten Dienste von Google und Co gibt es privatsphäre-freundliche und datensparsame Alternativen die wir unten vorstellen. Und sie werden täglich besser, auch weil sie mehr und mehr verwendet werden.

Was ist grundsätzlich von Smartphones zu halten? Sollte man die überhaupt benutzen? Wir finden: Smartphones sind praktische Helferlein, die Alltag und politische Organisierung erleichtern können. Richtig ist aber auch, dass Smartphones die universelle Wanze in der Hosentasche sein können und ein großes Helferlein für Ermittlungsbehörden und globale Werbekonzerne. Wer ohne Smartphone auskommt, gut. Für alle anderen soll diese Anleitung einen Ausweg aus dem Ganz-oder-Garnicht Denken liefern. Der Fokus des Artikels liegt darauf, das Smartphone von den Massenüberwachungs-Tools der großen Internet-Konzerne, vor allem Google, zu bereinigen und damit ein Mindestmaß an Privatsphäre wiederherzustellen. Schutz gegen gezielte Angriffe auf einzelne Smartphones, etwa durch Ermittlungsbehörden, ist nur am Rande Thema. Doch auch wenn es umfassende Sicherheit (gerade) im digitalen Leben nicht gibt, ist das kein Grund, den Kopf in den Sand zu stecken.

Wir beschreiben im Folgenden den Weg zu einem Smartphone, mit dem man (neben dem Telefonieren und SMS) problemlos und einigermaßen sicher Nachrichten schreiben, im Internet surfen, E-Mails lesen und navigieren kann. Nachdem das Thema lange nur für Nerds und mit viel Bastelei zu meistern war, ist es mittlerweile, mit ein wenig Computer-Kenntnissen, gar nicht mehr so schwer. Und wer es sich selbst nicht zutraut, fragt einfach mal im Freundeskreis um Hilfe.

WARUM DAS ALLES?

Gut 85 Prozent aller Smartphones und schätzungsweise 2 Milliarden Geräte weltweit laufen mit Android. Nahezu alle dieser Android-Smartphones haben Google Services installiert, mit deren Hilfe der Konzern massenhaft Daten wie Standortdaten, Browse- und Such-Historie, Anruf- und SMS-Protokolle, genutze Apps, etc. sammelt und dem persönlichen Google-Account zugeordnet speichert.

Eine Übersicht, welche Funktionen die Google Services bieten und was das mit (Abwesenheit von) Privatsphäre zu tun hat, liefert der Artikel »Geheime Kommandozentrale: Google Play-Dienste«: https://mobilsicher.de/hintergrund/geheime-kommandozentrale-google-play-dienste

Die gesammelten Informationen geben tiefe Einblicke in die privatesten Themen und Vorlieben jeder Einzelnen Google-User*in – und mit diesem Wissen von unvorstellbarem Ausmaß dem Konzern eine enorme Macht. Selbst wenn die gespeicherten Informationen nicht immer direkt einem Namen zugeordnet sind, kann aus ihnen leicht ermittelt werden, welche reale Person hinter dem betreffenden Profil steckt. Die einmal erhobenen Daten können jederzeit in falsche Hände geraten und für alles mögliche verwendet werden. Auch welchen Ermittlungsbehörden Zugriff auf die erhobenen Daten gegeben werden (müssen), kann sich schnell ändern – etwa durch neue Gesetze.

Was Google alles an privaten Daten speichert, fasst der Artikel »Welche Daten sammelt Google über mich?« zusammen: https://mobilsicher.de/hintergrund/was-sammelt-google-ueber-mich

Glücklicherweise lässt sich mittlerweile ein google-freies Android-Smartphone einrichten, das auch für Computer-Laien nutzbar ist, die wichtigsten Funktionen besitzt, regelmäßig mit Updates versorgt wird und ganz ohne die Google Services auskommt. Daher unser Appell: Probiert es aus! Macht eure und die Kommunikation eurer Kontakte ein wenig sicherer und entzieht sie der Massenüberwachung durch Google und Co.

Wer sich jetzt denkt: Aber Android selbst wird doch auch von Google entwickelt! – der hat Recht. Aber ein freies Betriebssystem dessen Entwicklung maßgeblich von Google finanziert wird zu nutzen, ist etwas anderes als die proprietären Dienste, die massenhaft personenbezogene Daten über euch und eure Kontakte an Google-Server senden: https://mobilsicher.de/hintergrund/wie-viel-google-steckt-in-android

EIN ALTERNATIVES ANDROID-BETRIEBSSYSTEM

Für ein google-freies Smartphone muss das gesamte Betriebssystem neu installiert werden. Die so genannten *G-Apps*, welche die Google Services beinhalten, sind so tief in das System installiert, dass sie nicht einfach gelöscht werden können.

Smartphone-Hersteller liefern ihre Geräte fast immer mit einer Android-Version (der so genannten »Stock ROM«) aus, bei der die *G-Apps* bereits installiert sind.

Glücklicherweise kann man auf den allermeisten Android-Smartphones eine andere Android Variante (so genannte »Custom ROM«) installieren. Dieser Vorgang überschreibt die aktuelle Android-Version.

Liste der unterstützten Geräte: https://wiki.lineageos.org/devices/

Wir empfehlen hier *LineageOS*, einen freien Nachbau von Android mit eigenen Sicherheits- und Privatsphäre-Erweiterungen. *LineageOS* wird durch ein großes Team von Entwickler*innen betreut und es werden regelmäßig Updates veröffentlicht – weshalb bekannte Sicherheitslücken schnell geschlossen werden. Außerdem legt das Community-Projekt großen Wert auf Transparenz, die Entwicklung passiert öffentlich nachvollziehbar und es gibt kein Unternehmen mit kommerziellem Interesse im Hintergrund.

Vor allem aber unterstützt *LineageOS* sehr viele Smartphone-Modelle. Da Smartphones unterschiedliche Hardware verwenden, gibt es leider keine Android Variante, die für alle Smartphones verfügbar ist. Man muss also schauen, ob *LineageOS* das eigene Smartphone unterstützt. Das kann man in der Liste der unterstützten Geräte nachsehen. Am besten wählt man das Smartphone beim (Second-Hand) Kauf direkt danach aus.

ALTERNATIVES ANDROID INSTALLIEREN



Bei der Installation von *LineageOS* unbedingt darauf achten, keine *GApps* zu installieren. Sonst holt ihr euch all die Google Services wieder auf euer Smartphone.

Die Installation des alternativen Android (z. B. *LineageOS*) überschreibt das bestehende Betriebssystem. Da die Installation je nach Smartphone-Modell unterschiedlich abläuft, sollten dafür die Installationshinweise auf den Seiten von LineageOS (in Englisch) gelesen und befolgt werden. Wir gehen im Folgenden nur grob die einzelnen Schritte der Installation durch:

1. **Backups:** Bevor mit der Installation begonnen wird, müssen alle noch benötigten Daten von dem Smartphone gesichert werden. Neben Bildern, Dokumenten und wichtigen Nachrichten gilt das auch für Kontakte und Kalender. Beginnt mit der Installation erst, wenn ihr sicher seid, dass keine wichtigen Daten mehr *ausschließlich* auf dem Smartphone sind.

2. **Computer vorbereiten:** Für die Installation wird ein Computer benötigt, an den das Smartphone per USB angeschlossen wird. Ideal ist ein Linux-Rechner, zur Not tut es auch ein MacOS oder Windows-Rechner. In jedem Fall muss *adb* (*Android Debug Bridge*) installiert sein. Wie das genau geht, findet ihr durch eine schnelle Suche nach »ADB in [Linux|Windows|Mac OS] installieren« raus.

3. **Recovery flashen:** Bevor ihr das eigentliche Android Betriebssystem installiert, muss das so genannte »Recovery System« überschrieben werden. Das ist ein kleines Programm, das zum Aktualisieren, Ändern und Reparieren des Betriebssystems dient und in einem extra Speicherbereich auf dem Smartphone liegt. Das bekannteste freie Recovery System ist TWRP. Die richtige Version für das Modell findet ihr in der Liste der Geräte.

https://twrp.me/

4. **Altes Betriebssystem löschen:** Aus dem zuvor installierten und gestarteten Recovery System heraus sollten alle Partitionen des Smartphones gelöscht werden. Das verhindert, dass Software aus dem alten Betriebssystem erhalten bleibt und möglicherweise im neu installieren System Schaden anrichtet. Das Löschen der Partitionen wird »wipen« genannt.

5. **LineageOS installieren:** Nachdem alle Partitionen gelöscht (gewiped) wurden, kann das neue *LineageOS* installiert werden. Die genaue Anleitungen zum Installieren von *LineageOS* findet sich auf der LineageOS-Seite zum Smartphone-Modell.

Liste der unterstützten Geräte:
https://wiki.lineageos.org/devices/

SPEICHER VERSCHLÜSSELN

!

Die Speicher-Verschlüsselung schützt nicht vor unbefugten Zugriffen bei laufendem Smartphone. Sie schützt nur, wenn das Smartphone ausgeschaltet ist. Trotzdem: vielleicht kann man das Gerät ja im richtigen Moment noch schnell ausschalten, oder man verliert es und der Akku wird leer, bevor es gefunden wird.

Wir empfehlen, den Daten-Speicher des Android-Betriebssystems zu verschlüsseln. Die Verschlüsselung dauert einmalig bis zu einer Stunde. Das Smartphone sollte dafür aufgeladen sein und am Strom hängen. Bei verschlüsseltem Smartphone muss man zum Starten des Smartphones ein Passwort eingeben, um den Speicher zu entschlüsseln.

Die Speicher-Verschlüsselung kann hier durchgeführt werden:

- Einstellungen ▶ Sicherheit ▶ Smartphone verschlüsseln ▶ Smartphone verschlüsseln

DIE APPS

Neben dem Betriebssystem sind es die Apps, die das Smartphone so nützlich machen. Wir beschreiben im Folgenden jeweils freie und privatsphäre-freundliche Alternativen für die wichtigsten Funktionen eines Smartphones.

APP STORE

Den App Store braucht man, um überhaupt Apps installieren zu können. **Folgende Einstellungen ist nötig um Apps aus alternativen App Stores installieren zu können:**

- Einstellungen ▶ Sicherheit ▶ Unbekannte Herkunft ▶ Einschalten

F-DROID: APP STORE FÜR OPEN SOURCE APPS

https://f-droid.org/

F-Droid ist **der** App Store für Freie Software. Wenn möglich, sollte Software aus diesem Store installiert werden. *F-Droid* muss einmalig manuell installiert werden. Dazu mit dem Browser des frisch installierten Android die *F-Droid* Seite aufrufen, »F-Droid herunterladen« auswählen und den Anweisungen folgen. Leider sind auch einige Open Souce Apps nicht im *F-Droid* Store verfügbar. Darunter so wichtige Apps wie *Firefox*, *Signal Messenger* und der *VLC Media Player*.

YALP STORE:
FREIER ZUGANG ZUM GOOGLE PLAY STORE

Um auch Apps installieren zu können, die nicht im *F-Droid Store* verfügbar sind, kann aus dem *F-Droid Store* die App *Yalp Store* installiert werden. Diese ermöglicht durch gefälschte Zugangsdaten einen freien Zugang zum Google Play Store.

Für alle aus dem *F-Droid Store* installierten Apps sollte im *Yalp Store* »Aktualisierungen ignorieren« eingestellt werden. Sonst überschreibt der *Yalp Store* die *F-Droid* Apps mit Versionen aus dem *Google Play Store*.

Mit dem *Yalp Store* kann man sich jede kostenlose App aus dem Play Store installieren. *Yalp* meldet auch automatisch, wenn Aktualisierungen für die installierten Apps verfügbar sind.

WEBBROWSER: FIREFOX

Wir empfehlen *Firefox* als Browser. *Firefox* wird von einer unabhängigen Stiftung entwickelt, die das Bedürfnis nach Privatsphäre zumindest einigermaßen ernst nimmt. Der *Firefox Browser* ist nicht in *F-Droid* verfügbar und muss mittels *Yalp Store* installiert werden.

Alternativ gibt es *Firefox Klar* (auch im *F-Droid Store*). Diese Firefox-Variante blockiert automatisch Werbung und Tracker und löscht die Browser-Historie beim Schließen.

Für mehr Privatsphäre sollten zusätzlich folgende Firefox AddOns installiert werden:

- *uBlock orgin* als Werbe-Blocker
- *Privacy Badger* als Schutz vor Tracking

https://addons.mozilla.org/en-US/firefox/addon/ublock-origin/

https://addons.mozilla.org/en-US/firefox/addon/privacy-badger17/

Außerdem sind folgende Einstellungen im Firefox hilfreich gegen Tracking:

- Datenschutz ▶ Aktivitäten nicht verfolgen
- Datenschutz ▶ Cookies
  ▶ Erlauben, aber nicht von Drittanbietern
- Suche ▶ *DuckDuckGo* (oder eine andere privatsphärefreundliche Suchmaschine wie *searx.me* oder *startpage.com* einstellen)

E-MAILS: K-9 MAIL

https://k9mail.github.io/

Wer auf seinem Smartphone E-Mails lesen und schreiben möchte, sollte dazu *K-9 Mail* verwenden. Die App kann über den *F-Droid Store* installiert werden.

https://www.openkeychain.org/

Für E-Mail Verschlüsselung kann optional noch *OpenKeychain* (aus dem *F-Droid Store*) installiert werden. Wobei man sich überlegen sollte, ob man seine PGP-Schlüssel auf dem Smartphone mit sich rumtragen möchte.

MESSENGER: SIGNAL UND CONVERSATIONS

Eine aktuelle Übersicht bietet der Artikel »Verschlüsselte Messenger: Threema, Signal, Telegram, WhatsApp«: https://mobilsicher.de/apps-kurz-vorgestellt/verschluesselt-kommunizieren-per-app

Das Thema sichere und datensparsame Messenger würde eigene ausführliche Artikel füllen. Hier werden zwei Messenger Apps empfohlen:

- **Signal** ist der beste uns bekannte Messenger der bei den Funktionen mit *Whatsapp*, *Telegram* und Co mithalten kann. *Signal* muss per *Yalp Store* installiert werden da er im *F-Droid Store* nicht verfügbar ist.
- **Conversations** ist der Beste Jabber/XMPP Client für Android. Jabber hat einige Vorteile gegenüber anderen Messengern. Der wichtigste ist: es braucht keine zentralen Server. User*innen können über verschiedene Jabber-Server verteilt miteinander kommunizieren. *Conversations* kann über den *F-Droid Store* installiert werden.



Noch ein kurzer Hinzweis: *Telegram* erachten wir nicht als sicher. Chats sind nicht standardmäßig Ende-zu-Ende verschlüsselt und Gruppenchats sind es niemals. Leider wird *Telegram* nach wie vor als vermeindlich »sichere Alternative« zu *Whatsapp* gehandelt – auch unter Linken. Die Genoss*innen von *Personal Data Defense Unit* haben im Artikel »Warum du den Messenger Telegram auf keinen Fall benutzen solltest« gute Argumente zusammengefasst: https://perdadub.blackblogs.org/2017/11/18/warum-du-den-messenger-telegram-auf-keinen-fall-benutzen-solltest/

Zusätzlich wollen wir noch auf *Silence* hinweisen, eine App zum Schreiben von verschlüsselten SMS. Wer auch ohne mobile Daten verschlüsselt kommunizieren will, sollte sich *Silence* anschauen. Die App kann über den *F-Droid Store* installiert werden.

KARTEN UND NAVIGATION: OSMAND (OFFLINE-KARTEN)

https://osmand.net/

Zur Navigation kann *OsmAnd* verwendet werden. Die App hat sehr umfangreiche Funktionen und ist zu Beginn etwas gewöhnungsbedürftig. Kartensätze müssen für die entsprechenden Regionen runtergeladen werden. Dafür funktioniert die Navi-

gation anschließend auch ohne Internet-Verbindung. Also z. B. im Ausland oder wenn man Mobilfunk-Verbindung und WLAN ausstellt.

Da alle Routen-Berechnungen und das Darstellen der Karten auf dem Gerät passieren ist die App etwas langsamer als man es vielleicht von *Google Maps* gewohnt ist. Dafür verrät man nicht jedes mal an einen großen Konzern (und potentiell andere Mithorchende), wo man gerade ist, wo man hin will und was man unterwegs macht.

Neben *OsmAnd* gibt es im *F-Droid Store* noch die recht neue App *Maps*. Sie ist leichter bedienbar als *OsmAnd* und hoffentlich in Zukunft eine gute Alternative.

OsmAnd lässt sich aus dem F-Droid Store installieren. Die Version dort hat mehr Features als die kostenlose Version im *Google Play Store*.

KALENDER UND KONTAKTE (OPTIONAL MIT CLOUD-ANBINDUNG)

Als Kalender empfehlen wir die App *Calendar* von *Simple Mobiletools* (verfügbar in *F-Droid*). Dieser Kalender funktioniert als rein lokaler Kalender, kann aber optional auch Kalender aus einer Cloud synchronisieren.

Am sichersten ist es, überhaupt keine Cloud Dienste für Funktionen auf dem Smartphone zu verwenden. Wenn man doch eine Cloud-Anbindung nutzen möchte, um Kontakte und/oder Kalender automatisch synchronisieren zu lassen, empfehlen wir dazu einen *Nextcloud* Account zu nutzen. Bei *systemli.org* sind eure E-Mail-Accounts mit einem von uns betreuten Nextcloud-Dienst verknüpft.

Für die Cloud-Anbindung kann die App *DAVdroid* aus dem *F-Droid Store* installiert und konfiguriert werden. In der App kann man auswählen, welche Adressbücher und Kalender synchronisiert werden sollen.

Zusätzlich kann man noch die App *Nextcloud* installieren. Sie bietet zum Beispiel die Funktion »Auto-Upload von Fotos«, die in einigen Situationen sehr praktisch sein kann.

PRO-TIPPS

WEITERFÜHRENDE LINKS ZU DATENSPARSAMKEIT UND SICHERHEIT UNTER ANDROID

- Security in-a-box: Basic Android Security Setup Guide: https://securityinabox.org/en/guide/basic-security/android/
- Digitalcourage: Befreien Sie Ihr Smartphone: https://digitalcourage.de/digitale-selbstverteidigung/befreien-sie-ihr-smartphone
- Free Software Foundation Europe: Befreien Sie Ihr Android: https://fsfe.org/campaigns/android/liberate.de.html

Hier noch ein paar Hinweise für Leute, die sich schon besser auskennen:

- **Updates für die Hardware Firmware:** Neben dem Android-Betriebssystem ist auf verschiedenen Chips eines Smartphones zusätzliche Software installiert, die so genannte Firmware. Hierfür gibt es keine freie Alternative und wir wissen nicht, was diese Firmware genau macht. Außerdem gibt es oftmals keine Sicherheits-Updates für sie.
- **Netzwerk-Aktivitäten der Apps überwachen:** Mit der App *Net Monitor* (aus dem *F-Droid Store*) kann man beobachten, welche Apps Verbindungen ins Internet aufbauen.
- **Smartphone rooten**: Häufig wird empfohlen, das Android-System zu rooten. Das bedeutet, auf dem System Administrator-Rechte zu erlangen. Da den Apps hiermit zusätzliche Rechte auf dem System eingeräumt werden, ist das ein potentielles Sicherheitsrisiko und sollte nur in Ausnahmefällen gemacht werden.
- **MicroG und Xposed:** Der freie *G-Apps* Nachbau *MicroG* kann hilfreich sein, wenn nicht auf die Funktionen der *G-Apps* verzichtet werden kann. *MicroG* zu installieren, reißt aber eine Sicherheitslücke ins System und sollte vermieden werden. Wer nicht auf *MicroG* verzichten kann, sollte sich dessen Fork (https://lineage.microg.org/) von *LineageOS* anschauen.

ÜBER SYSTEMLI.ORG

systemli.org ist ein 2003 gegründetes linkes Netzwerk und Technik-Kollektiv. Wir haben den Anspruch, sichere und vertrauenswürdige Kommunikationsdienste bereitzustellen. Das Projekt richtet sich insbesondere an politische Aktivist*innen und Menschen, die ein besonderes Datenschutzbedürfnis haben. Die Grundlage zur Erfüllung dieses Bedürfnisses bildet das Vertrauen der User*innen in uns. Wir schützen ihre Daten, indem wir sämtliche unserer Server und ihre Verbindungen verschlüsseln und keine unnötigen Verbindungsdaten speichern. Im Falle eines unbefugten Zugriffs bleiben die Daten so geschützt.

systemli.org ist aus politischen Strukturen erwachsen und begreift sich selbst als politisches Projekt. Wir sind nicht ausschließlich ein Technik-Kollektiv, welches kooperativ agiert, uns verbinden vor allem unsere politischen Ansprüche. Alle Mitglieder arbeiten »ehrenamtlich« für das Projekt. Wir sind als Kollektiv organisiert und treffen all unsere Entscheidungen gemeinsam.

Wir begreifen uns als:

- emanzipatorisch
- antifaschistisch
- antirassistisch
- antinationalistisch
- antikapitalistisch
- feministisch

Website: https://www.systemli.org
Kontakt: info@systemli.org

UNTERSTÜTZT UNS

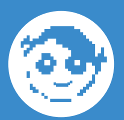
Alle Menschen für systemli.org arbeiten freiwillig und unbezahlt. Doch neben Zeit kostet das Bereitstellen unserer Dienste und Infrastruktur auch regelmäßig eine Menge Geld.

Damit wir unsere Dienste auch weiterhin anbieten können, sind wir auf eure Spenden angewiesen. Wir würden uns freuen, wenn jede Nutzer*in etwas Geld spenden oder gar einen Dauerauftrag einrichten könnte. Jede Spende hilft:

https://www.systemli.org/support-us.html

V.i.S.d.P.: N. Erd, Karl-Marx-Allee 45, 10178 Berlin | Titelbild: Marie Maerz / photocase.com

1. Auflage, April 2018



Was ist grundsätzlich von Smartphones zu halten? Sollte man die überhaupt benutzen? Wir finden: Smartphones sind praktische Helferlein, die Alltag und politische Organisierung erleichtern können. Richtig ist aber auch, dass Smartphones die universelle Wanze in der Hosentasche sein können und ein großes Helferlein für Ermittlungsbehörden und globale Werbekonzerne. Wer ohne Smartphone auskommt, gut. Für alle anderen soll diese Anleitung einen Ausweg aus dem Ganz-oder-Garnicht Denken liefern. Der Fokus des Artikels liegt darauf, das Smartphone von den Massenüberwachungs-Tools der großen Internet-Konzerne, vor allem Google, zu bereinigen und damit ein Mindestmaß an Privatsphäre wiederherzustellen. Schutz gegen gezielte Angriffe auf einzelne Smartphones, etwa durch Ermittlungsbehörden, ist nur am Rande Thema. Doch auch wenn es umfassende Sicherheit (gerade) im digitalen Leben nicht gibt, ist das kein Grund, den Kopf in den Sand zu stecken.